Japan Patent Office,
Unexamined Patent Application Publication No. H9-274584
PUBLICATION DATE: October 21, 1997

[Abstract of paragraph 10]

Fig.3 shows a location in which the security in files and directories are improved. An enciphering device 1 is defined by drive E; wherein, under root directory "E:¥" of drive E, includes directories "E:encript", "E:decript", file "PASSWORD", file "OFFSET", and file "COMPUTING EQUATION". File "PASSWORD" is a write only file; wherein, in a case that a user writes a password in the file, a controlling unit 18 checks the written password against the preset password. When the passwords are not in agreement, a file manipulation in enciphering device 1 is prohibited.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－274584

(43)公開日　平成９年(1997)10月21日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	12/00	５３７		Ｇ０６Ｆ	12/00	５３７Ｈ	
		５２０				５２０Ｊ	
	12/14	３２０			12/14	３２０Ｂ	

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平8－85382

(22)出願日　平成８年(1996)４月８日

(71)出願人　000006622
株式会社安川電機
福岡県北九州市八幡西区黒崎城石２番１号

(72)発明者　原　憲二
福岡県北九州市八幡西区黒崎城石２番１号
株式会社安川電機内

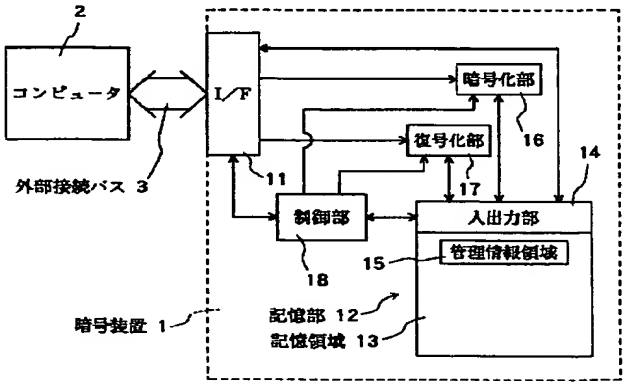
(74)代理人　弁理士　若林　忠

(54)【発明の名称】　暗号装置

(57)【要約】

【課題】特殊な操作を必要とせずに暗号化及び復号化を簡単な手順で行うことができ、かつ取り外し保管を容易にできる暗号装置を提供する。

【解決手段】コンピュータ２の外部接続バス３に着脱可能なインタフェース部１１と、記憶部１２と、データの暗号化を行う暗号化部１６と、暗号化されたデータの復号化を行う復号化部１７とを有し、コンピュータ２に接続されたときにコンピュータ３から見て階層的ファイル構成の外部記憶装置として扱われるように暗号装置１を構成する。暗号化用のディレクトリ及び復号化用のディレクトリを設け、暗号化用のディレクトリにファイル転送があったときには暗号化部１６で暗号化してからそのファイルを暗号化用のディレクトリに格納し、復号化用のディレクトリにファイル転送があったときにはそのファイルを復号化部１７で復号化してから復号化用のディレクトリに格納する。



1

【特許請求の範囲】

【請求項１】　コンピュータに接続されデータの暗号化及び復号化を実行する暗号装置であって、

前記コンピュータの外部接続バスに着脱可能なインタフェース手段と、

前記インタフェース手段に入出力するデータを記憶する記憶手段と、

データの暗号化を行う暗号化手段と、

暗号化されたデータの復号化を行う復号化手段とを有し、

前記コンピュータに接続されたときに前記コンピュータから見て階層的ファイル構成の外部記憶装置として扱われて第１のディレクトリ及び第２のディレクトリを有し、前記第１のディレクトリに対するデータ書き込みが指示された場合には前記暗号化手段によって当該データを暗号化して前記第１のディレクトリに格納し、前記第２のディレクトリに対するデータ書き込みが指示された場合には前記復号化手段によって当該データを復号化して前記第２のディレクトリに格納する、暗号装置。

【請求項２】　前記階層的ファイル構成でのファイルとしてパスワード書き込み用のファイルを有し、前記パスワード書き込み用ファイルに書き込まれたパスワードと予め設定されているパスワードとが対応しない場合には少なくとも前記第１のディレクトリ及び前記第２のディレクトリに対するファイル操作が禁止される請求項１に記載の暗号装置。

【請求項３】　前記階層的ファイル構成でのファイルとして暗号生成のための演算式に対するオフセットデータ書き込み用のファイルを有し、前記暗号化手段は前記オフセットデータ書き込み用のファイルからオフセットデータを読み出して前記演算式による暗号化結果に前記オフセットデータを加算して暗号化を行い、前記復号化手段は前記オフセットデータ書き込み用のファイルからオフセットデータを読み出して暗号化されたデータから前記オフセットデータを減算した後に前記演算式による復号化を行う請求項１または２に記載の暗号装置。

【請求項４】　暗号化及び復号化のための演算式を書き込むための演算式記憶領域を有し、前記演算式記憶領域から前記演算式を前記暗号装置の外部に読み出すことはできず、かつ、前記演算式記憶領域への書き込み回数が制限されている請求項１乃至３いずれか１項に記載の暗号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータで扱うデータの保全を図る装置に関し、特に、データの暗号化及び暗号化されたデータの復号化を行う暗号装置に関する。

【０００２】

【従来の技術】パーソナルコンピュータなどのコンピュータで取り扱うデータを保全する方法として、パスワードによりファイルへのアクセスを制限する方法があるが、この方法では、メモリあるいは外部記憶装置上にそのファイルのデータがそのままの形態で存在するので、不正にそのデータを読み出すことは不可能ではない。また、ネットワーク等を介して複数のコンピュータ間でデータをやり取りする場合、ネットワーク上での盗聴などに対する対策が必要となる。そこで、保全対象のデータを暗号化することが行われている。パーソナルコンピュータなどでデータの暗号化を行う場合、暗号化鍵や復号化鍵などのキーデータをパーソナルコンピュータ本体のハードディスクなどにそのまま記憶させておくことは、キーデータの配布やセキュリティ上の観点から、必ずしも好ましくない。また、暗号化のためにパーソナルコンピュータなどに対して付加するハードウェア量をできるだけ小さくすることが望まれる。そこで、特開昭６２－１３４６７９号公報には、キーデータを着脱可能なＩＣカード中に保管し、暗号化あるいは復号化に際してキーデータをＩＣカードからコンピュータ本体に読み込むようにした暗号文書作成読出装置が開示されている。また、特開昭６３－２４５０３５号公報には、復号化（平文化）するためのキーデータ論理回路を着脱可能なＩＣカード内に設け、暗号化されたデータがこのＩＣカードを介してループバックするようにすることにより、所望のデータが復号化される暗号通信装置が開示されている。

【０００３】

【発明が解決しようとする課題】しかしながら、上述した従来の装置では、暗号化あるいは復号化のために、通常のファイル操作とは異なる特別な操作手順が要求される。近年、コンピュータの操作環境のＧＵＩ（グラフィカル・ユーザ・インタフェース）化が進行し、マウス等のポインティングデバイスを用いたクリック動作あるいはドラッギング動作によって通常のファイル操作を行うことができるようになっているが、従来の暗号装置を用いる場合には、ユーザは複雑な操作手順を踏まえることを余儀なくされる。本発明の目的は、特殊な操作を必要とせずに暗号化及び復号化を簡単な手順で行うことができ、かつ取り外し保管を容易にできる暗号装置を提供することにある。

【０００４】

【課題を解決するための手段】本発明の暗号装置は、コンピュータに接続されデータの暗号化及び復号化を実行する暗号装置であって、前記コンピュータの外部接続バスに着脱可能なインタフェース手段と、前記インタフェース手段に入出力するデータを記憶する記憶手段と、データの暗号化を行う暗号化手段と、暗号化されたデータの復号化を行う復号化手段とを有し、前記コンピュータに接続されたときに前記コンピュータから見て階層的ファイル構成の外部記憶装置として扱われて第１のディレ

3

クトリ及び第２のディレクトリを有し、前記第１のディレクトリに対するデータ書き込みが指示された場合には前記暗号化手段によって当該データを暗号化して前記第１のディレクトリに格納し、前記第２のディレクトリに対するデータ書き込みが指示された場合には前記復号化手段によって当該データを復号化して前記第２のディレクトリに格納する。

【０００５】本発明の暗号装置は、階層的ファイル構成のパーソナルコンピュータなどを対象として、このコンピュータに対して取り外し可能なＩＣカードなどの形態を有するものであって、コンピュータ本体側からは階層的ファイル構成による外部記憶装置すなわち階層的ディレクトリによるファイルシステムとして見えるように構成されている。そして、暗号化のためのディレクトリと復号化のためのディレクトリとをこの暗号装置内に用意し、通常のファイル操作によってこれらのディレクトリに対してファイルの複写や移動が行われた際に、暗号化あるいは復号化が行われるようにしている。結局、通常のファイル操作によって所望のデータの暗号化や復号化を行うことができ、ユーザにとって分かりやすいユーザインタフェースを実現している。また、ＩＣカードなどの形態であるので、取り外し保管を容易に行うことができる。

【０００６】本発明においては、セキュリティのさらなる向上のため、ファイルシステムとしての暗号装置内にパスワード書き込み用のファイルを設け、このファイルに書き込まれたパスワードと予め設定されているパスワードとが対応しない場合には少なくとも暗号化用及び復号化用のディレクトリに対するファイル操作が禁止されるようにすることが好ましい。また、必要に応じて暗号強度を向上するため、暗号生成のための演算式に対するオフセットデータを書き込むファイルを設け、暗号化手段は演算式による暗号化結果にこのオフセットデータを加算して暗号化を行い、復号化手段は暗号化されたデータからこのオフセットデータを減算した後に演算式による復号化を行うようにするとよい。さらに、演算式自体もコンピュータ側から暗号装置内に書き込めるようにしてもよい。その場合には、演算式を書き込むための演算式記憶領域を例えばファイルとして設ければよい。ただし、セキュリティの向上のため、演算式記憶領域からは演算式を暗号装置の外部に読み出すことはできず、かつ、演算式記憶領域への書き込み回数を制限するようにするとよい。

【０００７】

【発明の実施の形態】次に、本発明の実施の形態について、図面を参照して説明する。図１は本発明の実施の一形態の暗号装置の構成を示すブロック図である。この暗号装置１は、パーソナルコンピュータなどの階層的ファイル構成によるコンピュータ２の外部接続バス３に対して取り外し可能に接続できるものであり、例えば、ＰＣ

4

ＭＣＩＡ(Personal Computer Memory Card International Association)規格によるＩＣカードとしての形態をとるものである。暗号装置１には、外部接続バス３との接続を行うためのインタフェース部１１と、インタフェース部１１に入出力するデータを記憶する記憶部１２と、データの暗号化を行う暗号化部１６と、暗号化されたデータの復号化を行う復号化部１７と、暗号装置１の全体の制御を行うための制御部１８とを有している。また、記憶部１２は、データが実際に記憶される領域である記憶領域１３と記憶領域１３に対してデータの入出力を行う入出力部１４とによって構成されており、また、記憶領域１３の内部には、ファイルアロケーションテーブルやルートディレクトリ領域などの管理情報領域１５が設けられている。この暗号装置１は、このように構成することにより、外部接続バス３を介してコンピュータ２に接続されたときに、階層的ファイル構成によるファイルシステムの外部記憶装置としてコンピュータ２から見えることになる。したがって、コンピュータ２で使用されているＯＳ（オペレーティングシステム）に応じ、通常のファイル操作によって、暗号装置１内にディレクトリやファイルを作成したり、ファイルを移動、複写したりすることができる。

【０００８】図２は、暗号装置１内のディレクトリやファイルの配置を典型的なＧＵＩ環境による表示画面で示した図である。ここでは、暗号装置１にはドライブ名「E:」が割り当てられおり、ドライブＥ：のルートディレクトリ「E:¥」の下に、２つのディレクトリ「E:¥encript」と「E:¥decript」が配置している。図においては、左右にそれぞれ表示窓が２１，２２が示されているが、左側の表示窓２１には、注目するドライブ（ここではドライブＥ：）のディレクトリツリーが表示され、右側の表示窓２２には、左側の表示窓２１内でユーザによって指定されたディレクトリ（図示破線で囲まれたディレクトリ）の内容が表示されている。上述した２つのディレクトリ「E:¥encript」と「E:¥decript」は、この暗号装置１を特徴付けるものであって、ディレクトリ「E:¥encript」に対してファイルが転送された場合には、暗号化部１６によってそのファイルが暗号化された後にディレクトリ「E:¥encript」に格納され、暗号化されたファイルがディレクトリ「E:¥decript」に転送された場合には、そのファイルが復号化されて平文となった後にディレクトリ「E:¥decript」に格納されるようになっている。実際には、これら各ディレクトリ「E:¥encript」,「E:¥decript」へのファイルの転送（移動や複写）があった場合、制御部１８でファイルの転送が検出され、制御部１８は、そのファイルのデータが暗号化部１６あるいは復号化部１７を経由するように、インタフェース部１１及び入出力部１４を制御する。具体的には、ディレクトリ「E:¥encript」と「E:¥decript」へのファイル転送に際しては、管理情報領域１５の特定のデータを書き換えるような命令がインタフェー

ス部１１を介して暗号装置１に入力するので、制御部１８がこの命令の入力の有無を監視し、そのような命令が入力した場合に暗号化部１６ないし復号化部１７をファイルのデータが通るようにすればよい。なお、ルートディレクトリ「E:¥」の下には、通常のファイルやディレクトリも配置することが可能であって、これら通常のファイルやディレクトリへのデータ転送、ファイル転送は、暗号化部１６や復号化部１７を介さずに行われる。

【０００９】暗号化部１６で暗号化のために使用する演算式、復号化部１７で復号化のために使用する演算式としては、例えば、米国標準局（ＮＢＳ:National Bureau ofStandard）によるＤＥＳ(Data Encryption Standard)などの暗号方法による演算式を用いることができる。以上のように暗号装置１を構成することにより、コンピュータ２での通常のファイル操作にしたがってファイルをディレクトリ「E:¥encript」あるいはディレクトリ「E:¥decript」に転送することによって、所望のファイルの暗号化あるいは復号化を行うことができる。例えば、平文によるテキストファイル「1250解説.TXT」をディレクトリ「E:¥encript」に転送すると、このファイルが暗号化されて「1250解説.CRP」が生成し、ディレクトリ「E:¥encript」内に格納される。ここで「CRP」は暗号化されたファイルを示す拡張子である。このようにしてディレクトリ「E:¥encript」に格納された暗号化後のファイルは、通常のファイル操作にしたがって他のドライブや他のディレクトリに移して保存することができ、また、ネットワークを介して他のコンピュータに転送することができる。同様に、暗号化されたファイル「1250解説.CRP」をディレクトリ「E:¥decript」に転送することにより、このファイルが復号化され、平文のテキストファイル「1250解説.TXT」が生成してディレクトリ「E:¥decript」に格納される。この復号化されたファイルも、ディレクトリ「E:¥decript」から自由に移すことができる。

【００１０】以上、本発明の基本的な実施の形態について説明したが、セキュリティの向上のため、この暗号装置１自体をパスワード保護したり、暗号化や復号化の演算式に対するオフセットデータを設けたり、演算式自体をコンピュータ２側から書き込めたりできるようにすることが好ましい。図３は、このようなセキュリティ向上の処置を施したした場合のファイル及びディレクトリの配置を示している。上述の場合と同様に、暗号装置１は外部記憶装置としてドライブＥ：で表わされているが、ドライブＥ：のルートディレクトリ「E:¥」の下には、ディレクトリ「E:¥encript」,「E:¥decript」の他に、ファイル「PASSWORD」,「OFFSET」,「演算式」が設けられている。このうち、ファイル「PASSWORD」は書き込み専用のファイルであって、ユーザがこのファイルにパスワードを書き込むと、制御部１８によって予め設定されているパスワードとの照合がなされ、一致していない場合には暗号装置１へのファイル操作が禁止される。

【００１１】ファイル「OFFSET」は、暗号化及び復号化の演算式に対するオフセットデータを指定するために使用される。このファイル「OFFSET」にオフセットデータが書き込まれている場合には、暗号化部１６はこのファイルからオフセットデータを読み出して演算式による暗号化結果にオフセットデータを加算し、オフセットデータが加算後の暗号化ファイルをディレクトリ「E:¥encript」に格納する。同様に復号化部１７は、復号化を行う際に、オフセットデータを読み出し、暗号化されたデータからこのオフセットデータを減算した後に演算式による復号化を行って、復号結果をディレクトリ「E:¥decript」に格納する。このようなオフセットデータを使用することにより、ＤＥＳなどで暗号化されたデータにさらに乱数列を被せることが可能になって、秘匿性がさらに向上する。オフセットデータとして無限乱数を用いれば、暗号を不正に解読することは完全に阻止される。

【００１２】ファイル「演算式」は、コンピュータ２側から演算式を書き込むために使用される。暗号化部１６及び復号化部１７は、ファイル「演算式」に書き込まれた演算式を用いて暗号化及び復号化を行う。この場合、制御部１８により、ファイル「演算式」の内容がこの暗号装置１の外部には読み出されないようにするとともに、ファイル「演算式」への書き込み回数をカウントし、規定回数以上の書き込みが行われないようにする。このように書き込み回数を制限することによって、他の暗号装置を用いて演算式の全てを試行することが不可能になり、セキュリティが向上する。

【００１３】

【発明の効果】以上説明したように本発明は、パーソナルコンピュータなどに対して取り外し可能なＩＣカードなどの形態であって階層的ファイル構成による外部記憶装置として扱える暗号装置とすることにより、通常のファイル操作と同様の操作手順で暗号化及び復号化を行えるようになるという効果がある。また、携帯性にも優れている。さらに、演算式やオフセットデータをユーザが決定できるようにすることにより、この暗号装置を多数市販した場合であっても個々の装置で演算式やオフセットデータを変更できるため、他の暗号装置を用いて不正に暗号の解読を行うことが不可能になる。結局、本発明によれば、簡単に使用でき、かつ秘匿性の高い暗号装置を提供できる。

【図面の簡単な説明】

【図１】本発明の実施の一形態の暗号装置の構成を示すブロック図である。

【図２】階層的ファイル構成での各ディレクトリ及び各ファイルの配置を説明する図である。

【図３】階層的ファイル構成での各ディレクトリ及び各ファイルの配置を説明する図である。

【符号の説明】

１　暗号装置

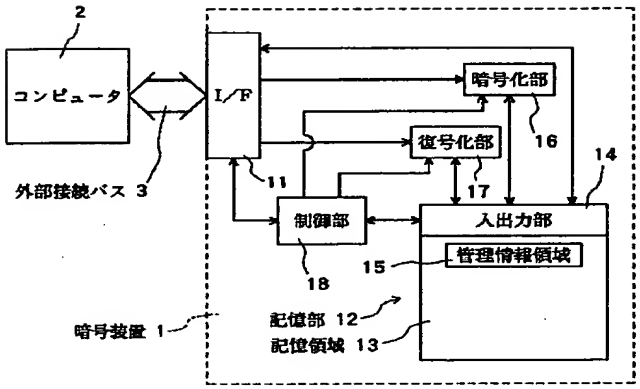
7

2　　コンピュータ
3　　外部接続バス
１１　　インタフェース部
１２　　記憶部
１３　　記憶領域
１４　　入出力部

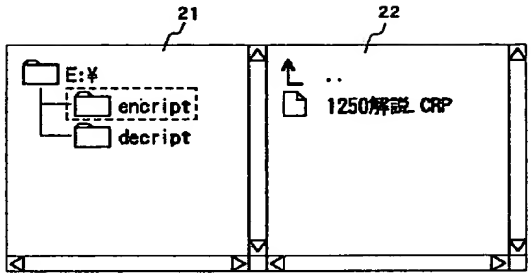
8

１５　　管理情報領域
１６　　暗号化部
１７　　復号化部
１８　　制御部
２１，２２　　表示窓

【図１】



【図２】



【図３】